Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 352 BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 februari 2015

Inleiding

In de brief van 7 november 2014 hebben wij uw Kamer geïnformeerd over de versterkingsagenda DigiD.[1] In het Algemeen Overleg van 11 november 2014 heeft uw Kamer verzocht om een overzicht van kosten die gemoeid zijn met de uitvoering van de versterkingsagenda (Kamerstuk 26 643, nr. 340). Dat overzicht wordt bij deze brief gegeven.

Uw Kamer vroeg daarnaast om een realistische inschatting van de meerkosten van het gebruik van mogelijke *aanvullende* beveiligingsmaatregelen op het basis betrouwbaarheidsniveau van DigiD en of er een businesscase onder de genoemde cijfers ligt. Ook dat overzicht wordt bij deze brief gegeven. Daarbij hoort wel de kanttekening dat in de begroting niet is voorzien in de uitvoering van één of meer van deze *aanvullende* beveiligingsmaatregelen.

Middels deze brief informeer ik uw Kamer tevens over de actuele stand van zaken met betrekking tot het oplossen van de onvolkomenheden op de naleving van de Beveiligingsnorm DigiD. Deze onvolkomenheden constateerde de Algemene Rekenkamer (AR) op verantwoordingsdag, 21 mei 2014. De AR constateerde dat de DigiD-omgeving, in 2013 niet volledig voldeed aan een deel van de normen van het Nationaal Cyber Security Centrum (NCSC) voor de beveiliging van webapplicaties.

In deze brief ga ik achtereenvolgens in op de kosten van de versterkingsagenda 2015, op de verschillende mogelijke aanvullende beveiligingsmaatregelen, op de kosten en baten afweging en sluit ik af met de voortgang bij het oplossen van de onvolkomenheden bij de naleving van de Beveiligingsnorm DigiD.

[1] Kamerstuk 26 643, nr. 332

kst-26643-352
ISSN 0921 - 7371
’s-Gravenhage 2015

Op dit moment kent DigiD de niveaus Basis en Midden. Voor Basis identificeren gebruikers zich met een gebruikersnaam en een wachtwoord; voor Midden identificeren gebruikers zich met een gebruikersnaam, een wachtwoord én een SMS-code.
DigiD Basis en DigiD Midden zijn van STORK niveau 2 resp. 2+.[2] Het voordeel van DigiD Midden boven DigiD Basis is dat daarmee in belangrijke mate wordt voorkomen dat burgers hun accountgegevens afstaan en dat daarmee het risico van «phishing» van accountgegevens kan worden tegengegaan. Deze praktijken behoren tot de grootste problemen binnen en buiten overheid bij voorkomen van fraude en oneigenlijk gebruik bij digitale dienstverlening.

Om DigiD op STORK niveau 3 te krijgen is face to face uitgifte van de accounts nodig; dat zou bijvoorbeeld kunnen via thuisbezorging of balie-uitgifte van activeringscodes. Deze methoden worden momenteel op beperkte schaal toegepast. Het thuisbezorgen vindt plaats in bepaalde postcode gebieden met een verhoogd risico en DigiD buitenland kent een vorm van balieuitgifte. Het hoogste betrouwbaarheidsniveau (STORK 4) is nog niet beschikbaar; om dat niveau te halen dient gebruik te worden gemaakt van gekwalificeerde elektronische certificaten.

Kosten Versterkingsagenda 2015

De versterkingsagenda is een samenstel van diverse extra acties die vanuit ICT en kostenperspectief de meest effectieve stappen zijn, zoals ik u in mijn brief van 7 november 2014 meldde. In totaal is hiervoor in 2015 een budget van 2,5 miljoen gereserveerd.[3] Daarnaast werkt het kabinet aan het realiseren van het eID Stelsel waarin private en publieke middelen kunnen worden ingezet voor authenticatie.

Alternatief DigiD midden

In de eerste plaats wordt een alternatief voor het redelijk kostbare DigiD Midden met SMS gerealiseerd, dat tegen lagere kosten op grote schaal kan worden toegepast. In februari start de bouw van de beoogde oplossing, medio 2015 wordt de beoogde oplossing beproefd in een pilot. Mocht de pilot succesvol blijken, dan zal besloten worden over uitrol en de daarmee samenhangende financiële consequenties. De kosten voor de pilot worden geraamd op ruim € 500.000. Mede door de pilot zal duidelijk worden wat de verdere investeringskosten, structurele beheerskosten en opbrengsten zijn.

Versterking DigiD met identiteitsdocument, niveau 3

Door enkele grote uitvoeringsinstanties worden in 2015 pilots uitgevoerd met het toepassen van een extra controle na het inloggen met DigiD. Die extra controle vindt plaats door het uitlezen van gegevens op de chip van een wettelijk identiteitsdocument, zoals de Nederlandse identiteitskaart en het rijbewijs. Daarmee wordt het mogelijk authenticaties met betrouwbaarheidsniveau STORK 3 uit te voeren. Mochten de pilots succesvol zijn, zal ik laten onderzoeken of, wanneer en tegen welke kosten deze methode overheidsbreed kan worden toegepast.

[2] STORK is een Europese classificatie die vier betrouwbaarheidsniveaus onderkent. Niveau 4 is het hoogste betrouwbaarheidsniveau.
[3] Dit bedrag komt bovenop de kosten van de reeds genomen maatregelen die in de brief van 7 november 2014 onder 1 en 2 zijn genoemd.

Publiek middel op hoogste betrouwbaarheidsniveau, niveau 4

In de brief over de voortgang van eID[4], die u 9 februari jl. hebt ontvangen, meld ik dat het kabinet het mogelijk en wenselijk acht in een publiek eID-middel te voorzien binnen het eID stelsel, waarmee authenticaties op het hoogste niveau mogelijk worden. Er worden momenteel voorbereidingen getroffen om kleinschalige pilots te starten met een publiek eID-middel. De financiering van deze kosten maakt onderdeel uit van de opdracht aan de Nationaal Commissaris voor de Digitale Overheid, zoals gemeld in bovengenoemde brief over de voortgang van eID.

ICT Beveiligingsassessments DigiD

Tot slot worden alle DigiD-gebruikende organisaties geacht, vóór 1 mei 2015, hun jaarlijkse rapportages over hun ICT-beveiligingsassessment DigiD op te leveren. De kosten voor de behandeling en beoordeling van rapporten, alsmede de correspondentie over de uitvoering van verbeterplannen worden voor 2015 begroot op ruim € 1 miljoen.

Raming kosten mogelijkeaanvullende beveiligingsmaatregelen

In de onderstaande tabel vindt u een overzicht van de kosten van het gebruik van een viertal mogelijke aanvullende maatregelen die, wanneer landelijk en algemeen toegepast, het betrouwbaarheidsniveau van DigiD verder zouden verhogen:
- het (verplicht) gebruik van DigiD Midden, momenteel met een SMS-code, bij alle digitale transacties met de op DigiD aangesloten organisaties;
- het aangetekend verzenden van alle brieven met activeringscodes bij nieuwe- en heraanvragen van DigiD's;
- de uitgifte van alle brieven met activeringscodes aan de balie van gemeenten;
- het overal thuisbezorgen van alle brieven met activeringscodes, zoals nu gebeurt in risicovolle postcodegebieden.

Aan de raming liggen de volgende aantallen ten grondslag:
- 158 miljoen authenticaties;
- 3 miljoen nieuwe- en heraanvragen.

Dit zijn de aantallen authenticaties en aanvragen in 2014.[5]

maatregel	aantal	kosten per stuk	totaal
basis authenticatie + sms (DigiD Midden)	158 miljoen	€ 0,10	€ 15.800.000
aangetekend verzenden activeringscodes	3 miljoen	€ 9,00	€ 27.000.000
balie-uitgifte activeringscodes	3 miljoen	€ 10,00	€ 30.000.000
thuisbezorging activeringscodes	3 miljoen	€ 23,50	€ 70.500.000

In de bijlage bij deze brief vindt u een specificatie van deze kostenramingen.

Bij verplicht gebruik van DigiD Midden zouden 5 miljoen burgers eerst hun DigiD-account moeten opwaarderen van niveau Basis naar niveau Midden. Daarmee zou, naast de bovenstaande 15,8 miljoen euro,

[4] Kamerstuk 26 643, nr. 349.
[5] Het aantal authenticaties verdubbelt momenteel elke twee jaar. Voor 2015 worden tussen de 205 en 250 miljoen authenticaties verwacht. Daarmee zouden de kosten voor DigiD Midden navenant stijgen.

eenmalig een bedrag van 5 miljoen gemoeid zijn voor het verzenden van de activeringcodes en het afhandelen van de reacties en vragen die daarop worden verwacht. (Vooropgesteld dat deze brieven via de «normale» post worden bezorgd, anders worden de kosten aanzienlijk hoger.)

Afweging extra kosten en baten

Uit opvragingen bij een aantal grote overheidsinstellingen blijkt dat het aantal schadegevallen direct gerelateerd aan het betrouwbaarheidsniveau van DigiD bij hen relatief laag is en dat hun schade naar schatting enkele tienduizenden euro's bedraagt. Vanuit financieel oogpunt wegen de geraamde aanvullende beveiligingskosten daarom op dit moment niet op tegen de schade die wordt opgelopen.
In bepaalde gevallen maken dienstaanbieders eigen keuzes in het doorvoeren van extra beveiligings- en controlemaatregelen. Dat past ook binnen de verantwoordelijkheid van elke publieke dienstaanbieder om het voor een digitale dienst of digitaal product passend betrouwbaarheidsniveau van authenticatie toe te passen. Zij kunnen ervoor kiezen om op eigen kosten voor één of meer diensten en/of producten DigiD Midden in te zetten. Zo is inloggen bijvoorbeeld bij de Dienst Uitvoering Onderwijs alleen mogelijk met DigiD Midden.

Bij het digitaal aanbieden van diensten en producten is het overheidsinstellingen er veel aan gelegen dat zowel veilig als klantvriendelijk te doen: zij trachten de drempel voor het gebruik – en daarmee de uitvoeringskosten – zo laag mogelijk te houden en tegelijk het risico op misbruik en/of oneigenlijk gebruik zo veel mogelijk te vermijden. Naast het voorkomen van schade hebben het imago van en het vertrouwen in DigiD hun onverdeelde aandacht. Maatregelen worden geselecteerd in overeenstemming met risico en belang. Aanvullend aan het gebruik van DigiD worden door de dienstaanbieders op eigen kosten mitigerende maatregelen getroffen om misbruik en oneigenlijk gebruik te voorkomen, zoals bij het wijzigen van adresgegevens of bankrekeningnummers.

Voortgang oplossen onvolkomenheden Beveiligingsnorm DigiD

Op verantwoordingsdag, 21 mei 2014, heeft de Algemene Rekenkamer (AR) haar verantwoordingsonderzoek aangeboden aan uw Kamer. De AR constateerde een aantal onvolkomenheden in de bedrijfsvoering van BZK. Eén van deze onvolkomenheden betreft de naleving beveiligingsnormen DigiD. De AR constateerde dat de DigiD-omgeving in 2013 niet volledig voldeed aan een deel van de normen van het Nationaal Cyber Security Centrum (NCSC) voor de beveiliging van webapplicaties.

In mijn bestuurlijke reactie op het verantwoordingsonderzoek 2014 heb ik maatregelen aangekondigd om te bereiken dat in 2014 de DigiD omgeving volledig zou voldoen aan die normen van het NCSC voor de beveiliging van webapplicaties. Daarnaast waren er al mitigerende maatregelen genomen, zodat er geen sprake is van een acuut beveiligingsrisico. Voorts heb ik in mijn brief van 9 september 2014[6] uw Kamer geïnformeerd dat medio mei 2014 een actieplan DigiD assessmentnormen is vastgesteld waarmee werd beoogd de bevindingen voor het einde van 2014 opgelost te hebben. Door middel van deze brief informeer ik u over de actuele stand van zaken rondom deze toezeggingen.

Gedurende en ultimo het jaar 2014 voldeed de DigiD omgeving nog niet volledig aan alle normen van het NCSC voor de beveiliging van webappli-

---

[6] Kamerstuk 31 490, nr.159.

caties. Er is in 2014 veel in gang gezet om verbeteringen in het beheer van DigiD te realiseren. Een taskforce bij de beheerorganisatie Logius, onderdeel van het Ministerie van BZK, heeft uitvoering gegeven aan het actieplan DigiD assessmentnormen. De geconstateerde bevindingen zijn grotendeels opgelost. Dit moet nog wel door een IT-audit[7] worden vastgesteld. Deze audit zal naar verwachting in het eerste kwartaal 2015 zijn afgerond. Er resteren thans nog twee bevindingen. Deze worden naar verwachting vóór de zomer van 2015 opgelost. Mede afhankelijk van het resultaat uit de audit is het mogelijk dat één oplossing nog verder moet worden aangescherpt. Mocht dit het geval zijn dan kan deze aanscherping pas op zijn vroegst eind 2015 plaatsvinden, omdat hiervoor eerst een ingrijpende wijziging in de ICT infrastructuur nodig is.
Naast het oplossen van de bevindingen naar aanleiding van afwijkingen van de norm, is een aantal onderzoeken uitgevoerd om na te gaan of er een materieel risico voor DigiD aan de orde is. Deze onderzoeken hebben geen noemenswaardige bevindingen opgeleverd.

De standaarden voor digitale beveiliging zijn continu in beweging en worden continu aangescherpt. DigiD wordt tegen meer normenkaders getoetst dan alleen de normen van het NCSC. Hierdoor is de situatie ontstaan dat er nieuwe bevindingen bij zijn gekomen op het beveiligingsgebied van DigiD. Het gaat om een groot aantal kleine, grote, urgente en minder urgente bevindingen van zeer diverse aard. De eerder genoemde taskforce zet zich in ook deze bevindingen op te lossen. Hiertoe zijn alle bevindingen geborgd in actieplannen. De voortgang daarvan wordt periodiek met de Auditdienst Rijk besproken, die intensief betrokken blijft bij het traject. Het is de verwachting dat, het traject met betrekking tot het oplossen van deze bevindingen, in 2015 ver zal komen. Het aantonen van de werking van al deze verbeteringen gaat van start nadat in opzet alles op orde is.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

[7] IT-auditing is het vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering.

BIJLAGE:

Specificatie raming mogelijke aanvullende beveiligingsmaatregelen

Basis authenticatie + SMS (DigiD Midden)

De prijs van een DigiD-authenticatie op niveau Midden is € 0,10. Dit bedrag is gebaseerd op de werkelijke kosten: afgerond 8 cent voor SMS kosten (inclusief opslag voor mislukte authenticaties en spraakberichten) en 2 cent aan service kosten.
Concreet is deze prijs inclusief:

- het versturen van een priority-SMS;
- incidentele gesproken berichten;
- incidentele berichten naar het buitenland;
- extra belasting van de DigiD Helpdesk en Servicecentrum;
- extra SMS in geval van een niet-geslaagde authenticatie.

Het aantal authenticaties in 2014 was 158 miljoen.
Als DigiD Midden voor alle transacties in 2014 zou zijn gebruikt, zouden de totale kosten derhalve € 15.800.000 bedragen.

Aangetekend verzenden activeringscodes

De kosten van het aangetekend verzenden van brieven met activeringscodes bedraagt naar schatting € 9,00. Naar schatting, omdat er nog geen ervaring met deze maatregel is opgedaan. Het is de prijs van Post NL voor aangetekend verzenden, met een kleine afronding omhoog voor het aansturen en beheren van dat proces.

Het aantal nieuwe- en heraanvragen DigiD, en daarmee het aantal verzonden brieven met activeringscodes, in 2014 was 3 miljoen.
Als alle brieven in 2014 aangetekend zouden zijn verzonden, zou daar dus € 27.000.000 mee zijn gemoeid.

Balie-uitgifte activeringscodes

Het fysiek uitreiken van een brief aan een (gemeente)balie, inclusief de identiteitsverificatie, kost volgens verschillende onderzoeken om en nabij € 10.00. Daarbij zijn directe kosten meegenomen, zoals te besteden tijd aan ontvangst, opslag, opzoeken en uitreiken van de brief, alsmede indirecte kosten verbonden aan het afgifteproces, zoals leiding, staf, planning, financiële ondersteuning en dergelijke.

Als alle brieven in 2014 aan de balie zouden zijn uitgereikt, zou dat dientengevolge € 30.000.000 hebben gekost.

Thuisbezorging activeringscodes

Het thuisbezorgen van brieven met activeringscodes kost, zoals het nu is ingericht met de Interdepartementale Post- en Koeriersdienst, gemiddeld € 23,50. Dat is een ervaringscijfer, waarbij uit de praktijk blijkt dat bij een derde van de brieven de bezorger meerdere keren aan de deur moet komen. Een bezorging sec kost € 18,00.

Als alle brieven met activeringscodes in 2014 aangetekend zouden zijn verzonden, was daarom € 70.500.000 uitgegeven.